1 Introduction

In this section, we make the necessary definitions to state the Quillen-Suslin theorem, aka Serre's Problem or Serre's Conjecture [1]. We mostly follow the notation and exposition in [Lam, 2006].

Definition 1.1 *An R -module M is* finitely generated *if there is $R^n \twoheadrightarrow M$, for some n. For a fixed ring R, we denote the collection of finitely generated R-modules by $\mathfrak{M}(R)$.*

Definition 1.2 *An R -module P is* projective *if there is some R-module Q such that $P \oplus Q$ is free.*

Definition 1.3 *The collection of finitely generated, projective R-modules will be denoted by $\mathfrak{B}(R)$.*

Here is an equivalent characterization.

Proposition 1.4 *An R-module P is projective iff every R-epimorphism onto P splits (i.e. has a right inverse).*

Proof Suppose that P is projective and let Q be some module such that $P \oplus Q$ is free. Further, suppose that we have some R-epimorphism $M \overset{\varphi}{\twoheadrightarrow} P$, where M is some R-module. We have some free basis for $P \oplus Q$, and we denote its elements by $\{(p_i, q_i) | i \in I\}$. Also we have the projection $\pi : P \oplus Q \twoheadrightarrow P$ defined by $\pi(p, q) = p$. Since φ is surjective, there are m_i such that $\varphi(m_i) = p_i$ for all $i \in I$. We define a map $\phi : P \oplus Q \to M$ by $\phi(p_i, q_i) = m_i$. In this way we see that $\varphi\phi = \pi$. But π obviously splits (has a right inverse), and therefore, so does φ.

Conversely, suppose that every R-epimorphism onto P splits. Denote by $R^{(P)}$ the free R-module on the elements of P. We have a canonical R-epimorphism $R^{(P)} \overset{\varphi}{\twoheadrightarrow} P$ which splits, by hypothesis. Therefore $R^{(P)} \cong P \oplus \ker \varphi$ so P is projective. ∎

The Quillen-Suslin theorem is

Theorem 1.5 (Quillen-Suslin) *Let k be a field and let $R = k[t_1, \ldots, t_n]$. Then every finitely generated, projective R-module is free.*

[1] However, Serre objected to the latter name.

Serre first posed the above theorem as a problem in [Serre, 1955].

Using the notation introduced in section 9, we can state this more concisely as $\mathfrak{B}(k[t_1, \ldots, t_n]) \subset \mathfrak{F}(k[t_1, \ldots, t_n])$.

In section 3 we will show $\mathfrak{B}(R) \subset \mathfrak{F}(R)$ for the case where R is a euclidean domain. Since $k[t]$ is a euclidean domain, we will then have shown Quillen-Suslin for the case $n = 1$.

We will spend some time to obtain a more concrete form of theorem 1.5. In fact it can be reduced to the statement that every right-invertible row with entries in $k[t_1, \ldots, t_n]$ can be completed, by adding more rows, to an invertible matrix. This is the standard way to reduce the statement, and was shown by Serre in [Serre, 1958]. We will, however, find it more convenient to work with the equivalent characterization in corollary 2.12. It is shown in section 2.5 that this is equivalent to the standard reduction mentioned above.

In section 4, we give a short proof of Quillen-Suslin (in the reduced form of corollary 2.12) by assuming Suslin's Lemma (lemma 4.1). In section 5, we prove Suslin's Lemma in an almost constructive way. The non-constructive part of the proof is contained in lemma 5.10. In section 6, we give a constructive proof of lemma 5.10. This proof is implemented in the Haskell programming language in Appendix A.

In the next section we will obtain a concrete condition on R such that $\mathfrak{B}(R) \subset \mathfrak{F}(R)$ is true.

2 A Concrete Condition

2.1 Outline

Our final task is to show that all finitely generated projective $k[t_1, \ldots, t_n]$-modules are free.

We will not quite accomplish that goal in this section, but we will find a concrete condition formulated in terms of matrices, which implies Quillen-Suslin. All later sections are then devoted to proving this condition constructively, and thus proving Quillen-Suslin.

The steps taken in this section are the following.

We will first relax the concept of freeness, by introducing the weaker concept of stable freeness.

Definition 2.1 *An R -module P is* stably free *if there are integers m and n such that $P \oplus R^m \cong R^n$.*

To make the following exposition a little less verbose, let us introduce the following notation, which will be used only in this section.

Notation The collection of free R-modules is denoted $\mathfrak{F}(R)$, and the collection of stably free R-modules is denoted $\mathfrak{F}_s(R)$

Then we will show that if M is a finitely generated, projective $k[t_1, \ldots, t_n]$-module, then M is stably free, that is; $\mathfrak{B}(k[t_1, \ldots, t_n]) \subset \mathfrak{F}_s(k[t_1, \ldots, t_n])$.

The next step is to find a sufficient condition on R such that $\mathfrak{B}(R) \cap \mathfrak{F}_s(R) \subset \mathfrak{F}(R)$.

Putting the above two conditions together for the case $R = k[t_1, \ldots, t_n]$ we will obtain a concrete condition, implying Quillen-Suslin.

2.2 Characterizing stably free modules

We now give a characterization of stably free modules. Note that, since every stably free module is also projective, we are characterizing $\mathfrak{B}(R) \cap \mathfrak{F}_s(R)$.

Proposition 2.2 *$P \in \mathfrak{F}_s(R)$ iff there is a split short exact sequence of the form*

$$0 \to P \to R^n \to R^m \to 0$$

for some m, n.

Proof P is stably free, so there are integers m and n such that $R^n \cong P \oplus R^m$. This is equivalent to the above short exact sequence splitting. ∎

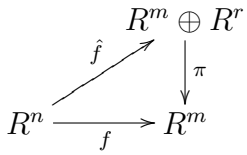
We can reinterpret this in more computationally friendly terms. As we just saw, we have $P \in \mathfrak{F}_s(R)$ iff $P \cong \ker(f : R^n \twoheadrightarrow R^m)$ where f splits i.e. has a right inverse. In other words, such a P is simply (isomorphic to) the kernel of some right invertible $m \times n$ matrix.

2.3 On the freeness of stably free modules

In this section, we characterize those $P \in \mathfrak{F}_s(R)$ which are also free. Note that, since stably free modules are projective, we are characterizing free modules in $\mathfrak{B}(R) \cap \mathfrak{F}_s(R) = \mathfrak{F}_s(R)$.

Proposition 2.3 *Suppose $P \cong \ker f$ where $f : R^n \twoheadrightarrow R^m$ is some split epimorphism. ($\Leftrightarrow P \in \mathfrak{F}_s(R)$).*

Then P is free iff there is some r and some isomorphism $\hat{f}$ such that the following diagram commutes



Proof Suppose P is free. Then $g : P \xrightarrow{\sim} R^r$ for some r. Also, since f splits, there is an isomorphism $\varphi : R^m \oplus P \xrightarrow{\sim} R^n$ with $\ker \varphi = 0 \oplus P$. Define $\hat{\varphi} : R^m \oplus P \to R^m \oplus R^r$ by $\hat{\varphi}(x, p) = (f\varphi(x, p), g(p))$. Clearly $\pi\hat{\varphi} = f\varphi$ so that $\pi\hat{\varphi}\varphi^{-1} = f$, i.e. we can take $\hat{f} = \hat{\varphi}\varphi^{-1}$. Suppose instead that $\hat{f}$ and r exists, such that the above diagram commutes. We have $f = \pi\hat{f}$, so $P \cong \ker f = \ker(\pi\hat{f}) \cong \ker \pi = 0 \oplus R^r \cong R^r$. ∎

We can interpret this in terms of matrices, as follows.

We have seen that $P \in \mathfrak{B}(R) \cap \mathfrak{F}_s(R)$ is simply the kernel of some right invertible $m \times n$ matrix M_f. Then the condition for freeness presented above is that there is an *invertible* $(m + r) \times n$ matrix $M_{\hat{f}}$ such that $M_f = M_\pi M_{\hat{f}}$. Here the $m \times (m + r)$ matrix M_π is the matrix projecting onto the first m coordinates.

Thus $M_f = M_\pi M_{\hat{f}}$ simply means that we can take the top m rows of the invertible matrix $M_{\hat{f}}$ and obtain our original matrix M_f.

However, it is better to think of it as saying that we can add rows onto M_f until we get an invertible matrix $M_{\hat{f}}$.

We have just shown the following interpretation.

Proposition 2.4 *Suppose that $P \in \mathfrak{B}(R) \cap \mathfrak{F}_s(R)$, so that P is isomorphic to the kernel of some right-invertible matrix M. Then P is free iff we can obtain an invertible matrix by adding rows to M.*

The above characterization only tells us if a single $P \in \mathfrak{B}(R) \cap \mathfrak{F}_s(R)$ is free.

We are ultimately interested in a condition that says that *every* $P \in \mathfrak{B}(R) \cap \mathfrak{F}_s(R)$ is free, i.e. to show $\mathfrak{B}(R) \cap \mathfrak{F}_s(R) \subset \mathfrak{F}(R)$.

A *necessary* condition for this to be the case is that, in particular, any right invertible row can be completed to an invertible matrix by adding rows.

This is also a *sufficient* condition, since a matrix being right invertible implies that each of its rows must be right invertible.

We have just shown the following theorem.

Theorem 2.5 *$\mathfrak{B}(R) \cap \mathfrak{F}_s(R) \subset \mathfrak{F}(R)$ iff every right invertible row vector with entries in R can be completed to an invertible matrix.*

In the next section, we will show that $\mathfrak{B}(k[t_1, \ldots, t_n]) \subset \mathfrak{F}_s(k[t_1, \ldots, t_n])$. Then the truth of the above theorem for $R = k[t_1, \ldots, t_n]$ will imply Quillen-Suslin.

Finally, we introduce a synonym for right invertible, which is common in the literature.

Definition 2.6 *A right invertible row vector over R is called a* unimodular row over R. *The set of all such rows is denoted $Um_n(R)$.*

2.4 Finitely generated, projective $k[t_1, \ldots, t_n]$-modules are stably free

The statement in the title is almost the Quillen-Suslin theorem. In light of theorem 2.5, the truth of this statement gives us a way to prove Quillen-Suslin in a very concrete way.

We will see that the result follows from Hilbert's syzygy theorem.

Theorem 2.7 (Hilbert's syzygy theorem) *Let $M \in \mathfrak{M}(k[t_1, \ldots, t_n])$. Then there is an exact sequence*

$$0 \to F_n \to \cdots \to F_0 \to M \to 0$$

where the F_i are all free and finitely generated.

For a proof, see for instance [Kunz, 1985, p. 208].

The exact sequence in Hilbert's syzygy theorem is called a *finite free resolution* for M.

Proposition 2.8 *Let M be a projective module with a finite free resolution. Then M is stably free.*

Proof We have

$$0 \to F_n \stackrel{\phi_n}{\to} \cdots \to F_0 \stackrel{\phi_0}{\to} M \to 0$$

where each F_i is free. We will proceed by induction on n. For $n = 0$ we are done, since in this case $M \cong F_0$ so that M is free. Now, consider $n > 0$. Denoting $M_1 = F_1/\ker \phi_1$, we have the following short exact sequence

$$0 \to M_1 \stackrel{\overline{\phi_1}}{\to} F_0 \stackrel{\phi_0}{\to} M \to 0$$

Since M is projective we see by proposition 1.4 that ϕ_0 splits. Therefore $F_0 = M_1 \oplus M$. Thus we are done if we can show that M_1 is stably free. But since M_1 is a summand of a free module, we see that M_1 is projective. We also have the following exact sequence

$$0 \to F_n \stackrel{\phi_n}{\to} \ldots F_2 \stackrel{\phi_2}{\to} F_1 \to M_1 \to 0$$

where again the last module, M_1, is projective.

By the induction hypothesis, we see that M_1 is stably free and so we are done. ∎

By Hilbert's syzygy theorem and the above proposition, we have trivially the following result.

Corollary 2.9 $\mathfrak{B}(k[t_1, \ldots, t_n]) \subset \mathfrak{F}_s(k[t_1, \ldots, t_n])$

Using theorem 2.5 and the above corollary, we obtain.

Corollary 2.10 *Quillen-Suslin is true iff every unimodular row with entries in $k[t_1, \ldots, t_n]$ can be completed to an invertible matrix.*

2.5 A slightly different condition

In the previous section, we reduced the proof of the Quillen-Suslin theorem to the problem of showing that any unimodular row over $k[t_1, \ldots, t_n]$ can be completed to an invertible matrix (corollary 2.10).

We will now reformulate this condition slightly, in preparation of the following sections.

Notation Let $\alpha, \beta \in R^n$ for some n. Then we write $\alpha \sim \beta$ if there is $M \in \mathrm{GL}_n(R)$ such that $\alpha M = \beta$. We write $\alpha \sim_G \beta$ if there is $M \in G$ such that $\alpha M = \beta$, where G is some subgroup of $\mathrm{GL}_n(R)$.

Proposition 2.11 *$\alpha \sim_G (1, 0, \ldots, 0)$ iff α can be completed to an element of G.*

Proof

$$\Rightarrow$$

Suppose $\alpha M = (1, 0, \ldots, 0)$. Write

$$M^{-1} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Where the $\beta_1, \ldots, \beta_n$ are rows of length n. Then let

$$M_\alpha = \begin{pmatrix} \alpha \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

Then $M_\alpha M = \mathbb{I}_n$ and thus by uniqueness of inverse, we have $M_\alpha = M^{-1} \in G$.

$$\Leftarrow$$

Using similar notation as above, suppose that

$$M_\alpha = \begin{pmatrix} \alpha \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} \in G$$

There is some $M_\alpha^{-1} \in G$ such that $M_\alpha M_\alpha^{-1} = \mathbb{I}_n$. This implies $\alpha M_\alpha^{-1} = (1, 0, \ldots, 0)$. ∎

Remark In light of corollary 2.10 and the above proposition, we see that the particular G does not really matter since corollary 2.10 states that the matrix by which our $\alpha \in \mathrm{Um}_n(R)$ is conjugate to $(1, 0, \ldots, 0)$ need only be *invertible*, i.e. an element of $\mathrm{GL}_n(R)$. Therefore we often write $\sim$ in place of $\sim_G$, and only remark on G when we find it worthwhile or interesting.

For clarity and future reference, we now combine corollary 2.10, and the above proposition.

Corollary 2.12 *Quillen-Suslin is true iff for any $f \in Um_n(k[t_1, \ldots, t_m])$ we have $f \sim (1, 0, \ldots, 0)$.*

This is the most important result of this section.

To summarize, a constructive proof of Quillen-Suslin amounts to an algorithm which, given a unimodular row f over $k[t_1, \ldots, t_m]$, produces an invertible matrix $G \in \mathrm{GL}_n(k[t_1, \ldots, t_m])$ such that $fG = (1, 0, \ldots, 0)$.

3 The Case of Euclidean Domains

In this section, we prove the Quillen-Suslin theorem in the case where $n = 1$ so that the base ring $R = k[t]$ is a euclidean domain. The proof basically reduces to the euclidean algorithm. This result will be used to give the general proof later on.

Proposition 3.1 *Let R be a euclidean domain and let $\alpha = (a_1, \ldots, a_n) \in R^n$. Then $\alpha \sim_G (g, 0, \ldots, 0)$ where $G = EL_n(R)$ and $g = \gcd(a_1, \ldots, a_n)$.*

Proof We can apply the ordinary euclidean algorithm to $(a_1, \ldots, a_n)$, which is just a sequence of elementary transformations transforming $(a_1, \ldots, a_n)$ into $(g, 0, \ldots, 0)$. The product of these elementary transformations is an element in $\Gamma \in \mathrm{EL}_n(R)$ such that $(a_1, \ldots, a_n)\Gamma = (g, 0 \ldots, 0)$. ∎

Corollary 3.2 *Let R be a euclidean domain and let $\alpha = (a_1, \ldots, a_n) \in Um_n(R)$. Then $\alpha \sim_G (1, 0, \ldots, 0)$ where $G = EL_n(R)$.*

Proof The fact that α is unimodular implies that $\gcd(a_1, \ldots, a_n)$ is a unit. Thus, by proposition 3.1, there is $\Gamma \in \mathrm{EL}_n(R)$ such that $\alpha\Gamma = (1, 0, \ldots, 0)$. ∎

By corollary 2.10, this implies Quillen-Suslin for the case $n = 1$.

4 A proof of Quillen-Suslin using Suslin's Lemma

4.1 Outline

In this section we will put together a proof of the Quillen-Suslin theorem. More specifically, we will prove the condition given in corollary 2.12 for the particular case of $R = k[t_1, \ldots, t_m]$. Namely that if we have a unimodular row $f = (f_1, \ldots, f_n) \in \mathrm{Um}_n(k[t_1, \ldots, t_m])$ then $f \sim (1, 0, \ldots, 0)$. By the mentioned corollary, this implies Quillen-Suslin.

Note that the following is a constructive argument, assuming Suslin's lemma. Suslin's Lemma will be proved in the sections following this one.

4.2 Proving Quillen-Suslin using Suslin's Lemma

We first state Suslin's Lemma.

Lemma 4.1 (Suslin's Lemma) *Let R be a commutative ring and suppose $f \in Um_n(R[t])$. Suppose further that either*

- $n = 1, 2$
- $n \geq 3$ *and f has a monic component.*

Then $f(t) \sim f(0)$.

As noted above, we will give the proof later, of course *without using any of the results we derive from it here.*

Lemma 4.2 (Nagata) *Let $f \in k[t_1, \ldots, t_m]$. Then there is an automorphism $\varphi : k[t_1, \ldots, t_m] \to k[t_1, \ldots, t_m]$ such that $\varphi(f)$ is monic with respect to t_1.*

This is a standard result. For instance, see [Lam, 2006, p. 103] for a constructive proof.

By Nagata and Suslin's lemma, we have the following corollary.

Corollary 4.3 *Let $R = k[t_1, \ldots, t_m]$ and $f \in Um_n(R[t])$. Then $f(t) \sim f(0)$*

Theorem 4.4 *Let $f \in Um_n(k[t_1, \ldots, t_m])$. Then $f \sim (1, 0, \ldots, 0)$.*

Proof We proceed by induction on m. The base case, $m = 1$, has already been taken care of. (This is the case of a euclidean domain, and so we are done by corollary 3.2.)

To take the induction step, we use the above corollary. ∎

We have now proved Quillen-Suslin using Suslin's Lemma. The remainder of this paper is devoted to proving Suslin's Lemma.

5 Proving Suslin's Lemma

5.1 Outline

In this section, we will complete the proof of the Quillen-Suslin theorem by giving a proof of Suslin's lemma (lemma 4.1). The proof given in this section will not be constructive, but we will modify it in a later section in order to obtain a constructive argument.

Suslin's Lemma says that, if $f \in \mathrm{Um}_n(R[t])$ then $f(h) \sim f(h')$ for any $h, h' \in R[t]$. In the case of Quillen-Suslin, we have $R = k[t_1, \ldots, t_m]$ but there is no reason to restrict ourselves to this case.

Notation $I_{f,G} = \{c \in R | h - h' \in \langle c \rangle [t] \Rightarrow f(h) \sim_G f(h')\}$ for some subgroup G of $\mathrm{GL}_n(R[t])$. If we drop the G and only write I_f then $G = \mathrm{GL}_n(R[t])$ is implied.

Suslin's Lemma then says that $f \in \mathrm{Um}_n(R[t]) \Rightarrow I_f = R$. It is a pleasant fact that I_f is an ideal:

Proposition 5.1 *Let R be some ring, $f \in R[t]^n$ and G some subgroup of $GL_n(R[t])$. Then the set $I_{f,G} = \{c \in R | g - g' \in \langle c \rangle [t] \Rightarrow f(g) \sim_G f(g')\}$ is an ideal.*

Proof Suppose $a, b \in I_{f,G}$, and let us show that for any $x, y \in R$ we have $ax + by \in I_{f,G}$. Let $g - g' = (ax + by)h$ for some $h \in R[t]$. Rearrange to obtain $g - axh = g' + byh$. Then we have

$$f(g) \sim_G f(g - axh) = f(g' + byh) \sim_G f(g')$$

where we first used $a, b \in I_{f,G}$. Now since $\sim_G$ is an equivalence relation, we have obtained $f(g) \sim_G f(g')$ and so we are done. ∎

We will show that I_f contains a unit if f is a unimodular row. We will do this by showing that for every maximal ideal $\mathfrak{m} \subset R$, there exists $c \in I_f - \mathfrak{m}$. Finding this c is the tricky part.

It turns out to be quite easy to prove Suslin's lemma for the cases $n = 1, 2$. The $n = 2$ case will also be used in the proof for $n \geq 3$.

5.2 Suslin's Lemma for $n = 1, 2$

We first deal with the case $n = 1$. Since $f \in \mathrm{Um}_1(R[t])$ simply means that f is invertible, there is some $g \in R[t]$ such that $f(t)g(t) = 1$. Given any $h, h' \in R[t]$, we can change variables, and get $f(h)g(h) = 1$ and $f(h')g(h') = 1$. Thus $f(h)(g(h)f(h')) = f(h')$. (Note that $g(h)f(h')$ is invertible, as required in Suslin's lemma.)

Now we deal with the case $n = 2$.

Lemma 5.2 *Let R be a commutative ring and suppose that $f = (f_1, f_2) \in R[t]^2$. Then $c \in \langle f_1, f_2 \rangle \cap R \Rightarrow c \in I_{f,G}$. (Here $G = SL_2(R[t])$)*

Proof We must show that given any $h, h' \in R[t]$ such that $h' = h + ck$ for some $k \in R[t]$, there is a matrix $M \in \mathrm{SL}_2(R[t])$ such that $f(h)M = f(h')$.

Introduce $\phi(x, y, z)$ and $\psi(x, y, z)$ such that

$$\begin{array}{l} f_i(x + yz) = f_i(x) + z\phi_i(x, y, z) \\ g_i(x + yz) = g_i(x) + z\psi_i(x, y, z) \end{array} \text{ for } i = 1, 2$$

Now define

$$M(x, y, z) = \begin{pmatrix} 1 + g_1(x)\phi_1(x, y, z) + f_2(x)\psi_2(x, y, z) & g_1(x)\phi_2(x, y, z) - f_2(x)\psi_1(x, y, z) \\ g_2(x)\phi_1(x, y, z) - f_1(x)\psi_2(x, y, z) & 1 + g_2(x)\phi_2(x, y, z) + f_1(x)\psi_1(x, y, z) \end{pmatrix}$$

We claim that $M(h, k, c)$ is the desired matrix. To check this, let us compute $f(x)M(x, y, z)$ and $\det M(x, y, z)$. We suppress arguments to avoid clutter.

$$f(x)M(x, y, z) =$$

$$(f_1, f_2) \begin{pmatrix} 1 + g_1\phi_1 + f_2\psi_2 & g_1\phi_2 - f_2\psi_1 \\ g_2\phi_1 - f_1\psi_2 & 1 + g_2\phi_2 + f_1\psi_1 \end{pmatrix} =$$

$$= (f_1 + (f_1g_1 + f_2g_2)\phi_1, f_2 + (f_1g_1 + f_2g_2)\phi_2) =$$

$$= (f_1 + c\phi_1, f_2 + c\phi_2)$$

Evaluating at $(x, y, z) = (h, k, c)$ we get $f(h)M(h, k, c) = f(h + ck) = f(h')$, as desired. Now we compute $\det M(x, y, z)$.

$$\det M(x, y, z) =$$

$$= (1 + g_1\phi_1 + f_2\psi_2)(1 + g_2\phi_2 + f_1\psi_1) - (g_2\phi_1 - f_1\psi_2)(g_1\phi_2 - f_2\psi_1) =$$

$$= 1+g_1\phi_1+f_2\psi_2+g_2\phi_2+f_1\psi_1+(g_1\phi_1+f_2\psi_2)(g_2\phi_2+f_1\psi_1)-(g_2\phi_1-f_1\psi_2)(g_1\phi_2-f_2\psi_1) =$$

$$= \begin{array}{c} 1 + g_1\phi_1 + f_2\psi_2 + g_2\phi_2 + f_1\psi_1 + g_1g_2\phi_1\phi_2 + f_1g_1\phi_1\psi_1 + f_2g_2\phi_2\psi_2 + f_1f_2\psi_1\psi_2 \\ - [g_1g_2\phi_1\phi_2 - f_2g_2\phi_1\psi_1 - f_1g_1\phi_2\psi_2 + f_1f_2\psi_1\psi_2] \end{array} =$$

$$= \begin{array}{c} 1 + g_1\phi_1 + f_2\psi_2 + g_2\phi_2 + f_1\psi_1 + g_1g_2\phi_1\phi_2 + f_1g_1\phi_1\psi_1 + f_2g_2\phi_2\psi_2 + f_1f_2\psi_1\psi_2 \\ -g_1g_2\phi_1\phi_2 + f_2g_2\phi_1\psi_1 + f_1g_1\phi_2\psi_2 - f_1f_2\psi_1\psi_2 \end{array} =$$

$$= 1+g_1\phi_1+f_2\psi_2+g_2\phi_2+f_1\psi_1+f_1g_1\phi_1\psi_1+f_2g_2\phi_2\psi_2+f_2g_2\phi_1\psi_1+f_1g_1\phi_2\psi_2 =$$

$$= 1 + g_1\phi_1 + f_2\psi_2 + g_2\phi_2 + f_1\psi_1 + (f_1g_1 + f_2g_2)\phi_1\psi_1 + (f_1g_1 + f_2g_2)\phi_2\psi_2 =$$

$$= 1 + (f_1\psi_1 + g_1\phi_1 + c\phi_1\psi_1) + (f_2\psi_2 + g_2\phi_2 + c\phi_2\psi_2)$$

Evaluating at $z = c$ we obtain

$$\det M(x, y, c) = 1 + \xi_1(x, y, c) + \xi_2(x, y, c)$$

where $\xi_i(x, y, z) = f_i(x)\psi_i(x, y, z) + g_i(x)\phi_i(x, y, z) + z\phi_i(x, y, z)\psi_i(x, y, z)$. Now note that $z\xi_i(x, y, z) = f_i(x+yz)g_i(x+yz)-f_i(x)g_i(x)$ so that $z(\xi_1(x, y, z)+\xi_2(x, y, z)) = c - c = 0 \Rightarrow \xi_1(x, y, z) + \xi_2(x, y, z) = 0$. Thus we may conclude $\det M(h, k, c) = 1$. ∎

Remark For a more intuitive proof, one can assume that R is an integral domain. See [Lam, 2006, Lemma 1.2, p. 100] for such a proof. As Lam points out, and as is evident in the above proof, there is no need to assume that R is an integral domain, or even that c is not a zero divisor.

Suslin's lemma for $n = 2$ now follows as a corollary: if $f = (f_1, f_2)$ is unimodular, then we obtain $c = 1 \in \langle f_1, f_2\rangle \cap R$. By the above lemma, we obtain $f(h) \sim_{\mathrm{SL}_2(R[t])} f(h')$ for any $h, h' \in R[t]$.

The rest of this section is devoted to proving Suslin's Lemma for the other cases as well, namely $n \geq 3$.

5.3 The extension $R \subset R[t]/\langle f \rangle$

In this subsection, we let $f \in R[t]$ be a monic polynomial of degree d over R.

Let us denote $S = R[t]/\langle f \rangle$ in this section.

It is clear that S is a finitely generated free R-module with basis $1, t, t^2, ..., t^{d-1} \in S$. For any $g \in S$, consider the map $\mu_g : S \to S$ defined by $\mu_g(h) = gh$. This is an R-linear map, and can therefore be represented by a $d \times d$ matrix with entries in R. Note then that $\det \mu_g \in R$.

Therefore, the following "norm function" is well defined.

Definition 5.3 *$N_f : S \to R$ defined by $N_f(g) = \det \mu_g$.*

Remark $N_f(g)$ is usually denoted as $\mathrm{Res}(f, g)$ and called the resultant of f and g. Note also that in the following sections, we will view N_f as a map from $R[t]$ rather than S, in a natural way. In this case, given $g, h \in R[t]$ such that $g - h \in \langle f \rangle$, we obtain $\mu_g = \mu_h$ and consequently $N_f(g) = N_f(h)$.

Proposition 5.4 *Let I be an ideal of R. Then if $g \in IS$, the matrix M_g corresponding to μ_g has entries in I.*

Proof Write $g(t) = a_n t^n + \cdots + a_0$ where $a_i \in I$. Then we see that $M_g = a_n M_{t^n} + \cdots + a_0 M_1$. Thus M_g has entries in I since each a_i is in I. ∎

The characteristic polynomial of μ_g will help us to prove things about the norm function.

Definition 5.5 *Let $g \in S$. Then denote the matrix corresponding to μ_g by M_g. We define $\chi_g(x) = \det(x\mathbb{I} - M_g) \in S[x]$. We call χ_g the* characteristic polynomial *corresponding to g.*

We summarize some important properties in the following proposition.

Proposition 5.6 *Let I be an ideal of R and let $g \in IS$. Then $\chi_g(x)$ is monic of degree d, with constant coefficient equal to $(-1)^d N_f(g)$. That is; $\chi_g(x) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + (-1)^d N_f(g)$. We also have $N_f(g), a_1, \ldots, a_{d-1} \in I$, and $\chi_g(g) = 0$.*

Proof The leading term of $\chi_g(x)$ clearly comes from the product of the entries on the diagonal of $x\mathbb{I} - M_g$, which is $\prod_{i=1}^{d}(x - m_{ii}) = x^d + \ldots$. Thus we see that $\chi_g(x)$ is monic and has degree d.

The constant coefficient of $\chi_g(x)$ is $\chi_g(0) = \det(-M_g) = (-1)^d N_f(g)$.

Thus we can write $\chi_g(x) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + (-1)^d N_f(g)$.

By proposition 5.4, M_g has entries in I. Thus the off-diagonal entries of $x\mathbb{I} - M_g$ are in I. The off-diagonal entries of $x\mathbb{I} - M_g$ will divide terms in $\det(x\mathbb{I} - M_g)$ of strictly lower degree than d. Therefore $N_f(g), a_1, \ldots, a_{d-1} \in I$. In order to prove $\chi_g(g) = 0$, we appeal to the Cayley-Hamilton theorem, which implies that $\chi_g(\mu_g) = 0$. But $\chi_g(\mu_g) = \mu_{\chi_g(g)}$, so we obtain $\mu_{\chi_g(g)} = 0$. This implies $\chi_g(g) = 0$. ∎

Proposition 5.7 *Let g be any element of S. Then we have that $N_f(g) \in R \cap \langle g \rangle$.*

Proof By proposition 5.6, we have $\chi_g(g) = g^d + a_{d-1}g^{d-1} + \cdots + a_1 g + (-1)^d N_f(g) = 0$. Thus $N_f(g) \in R \cap \langle g \rangle$. ∎

Lemma 5.8 *Let $I \subset R$ be an ideal of R, and let $g \in IS$. Then $N_f(1+g) \in 1 + I$.*

Proof Let M_g be the matrix corresponding to μ_g. The identity matrix corresponds to μ_1. Clearly μ_{1+g} is represented by $M_{1+g} = \mathbb{I} + M_g$. By proposition 5.4, all entries of M_g are in I. Thus we get $N_f(1+g) \equiv N_f(1) \equiv 1 \mod I$. ∎

5.4 A non-constructive proof

Lemma 5.9 *Let $f = (f_1, ..., f_n) \in R[t]^n$ and suppose that $\Gamma \in EL_{n-1}(R[t])$ is such that $(g_2, ..., g_n) = (f_2, ..., f_n)\Gamma$ where there is $c \in \langle f_1, g_2 \rangle \cap R$. Then $c \in I_f$.*

Proof We must show that if $h \equiv h' \mod \langle c \rangle[t]$, then $f(h) \sim f(h')$. This is done in the following sequence of steps.

$f(h)$	$\sim_{\mathrm{EL}_n}$	$(f_1(h), g_2(h), g_3(h), \ldots, g_n(h))$	using Γ
	$\sim_{\mathrm{EL}_n}$	$(f_1(h), g_2(h), g_3(h'), \ldots, g_n(h'))$	by the derivation below
	$\sim_{SL_n}$	$(f_1(h'), g_2(h'), g_3(h'), \ldots, g_n(h'))$	using lemma 5.2, with c as given
	$\sim_{\mathrm{EL}_n}$	$(f_1(h'), f_2(h'), f_3(h'), \ldots, f_n(h'))$	using Γ again
	$=$	$f(h')$	

We now prove the second step. It clearly follows if $g_i(h) - g_i(h') \in \langle f_1(h), g_2(h)\rangle$, for $3 \geq i \geq n$. Begin by noting that $g_i(h) - g_i(h') \in \langle h - h'\rangle$ (using the general fact that $(x-y)|(x^n - y^n)$). But by choice we have $h - h' \in \langle c\rangle[t]$, and furthermore we have that $c \in \langle f_1, g_2\rangle$. Putting these facts together we obtain $g_i(h) - g_i(h') \in \langle h - h'\rangle \subset \langle c\rangle[t] \subset \langle f_1(h), g_2(h)\rangle$. ∎

Note that the above proof is constructive.

Now we can give a non-constructive proof of Suslin's lemma. By Nagata (lemma 4.2), we may assume that f_1 is monic without loss of generality.

Lemma 5.10 *Suppose that $f \in Um_n(R[t])$ is a unimodular row with f_1 monic and $n \geq 3$. Then we have*

$$1 \in \langle N_{f_1}(((f_2, \ldots, f_n)\Gamma)_1) \mid \Gamma \in EL_{n-1}(R[t])\rangle$$

Proof We give a proof by contradiction. The contradiction to the hypothesis implies that $1 \notin L$ where $L = \langle N_{f_1}(((f_2, \ldots, f_n)\Gamma)_1) \mid \Gamma \in \mathrm{EL}_{n-1}(R[t])\rangle$. Then there is some maximal ideal $\mathfrak{m} \subset R$ of R such that $L \subset \mathfrak{m}$ Now note that $(R/\mathfrak{m})[t]$ is a euclidean domain. Therefore, applying proposition 3.1 to the last $n-1$ components, we see that there is $\overline{\Gamma} \in \mathrm{EL}_{n-1}((R/m)[t])$ such that $((\overline{f}_2, \ldots, \overline{f}_n)\overline{\Gamma})_1 = \overline{g}$ where $\overline{g} = \gcd(\overline{f}_2, \ldots, \overline{f}_n)$. We have $\overline{1} \in \langle \overline{f}_1, \overline{g}\rangle$ in $(R/\mathfrak{m})[t]$. Now lift $\overline{\Gamma} \in \mathrm{EL}_{n-1}((R/\mathfrak{m})[t])$ to some $\Delta \in \mathrm{EL}_{n-1}(R[t])$. Concretely, we have $h_1 f_1 + h_2 g \in 1 + \mathfrak{m}[t]$ where $g = ((f_2, \ldots, f_n)\Delta)_1$. Taking the norm with respect to f_1 and using lemma 5.8, we obtain $N_{f_1}(h_2)N_{f_1}(g) \in 1 + \mathfrak{m}$. Therefore $N_{f_1}(g) \notin \mathfrak{m}$. But of course $N_{f_1}(g) = N_{f_1}(((f_2, \ldots, f_n)\Delta)_1) \in L$ and so L is not a subset of $\mathfrak{m}$, which is our contradiction. ∎

This proof is non-constructive for two reasons; firstly it is a proof by contradiction, and secondly it asserts the existence of a maximal ideal, which requires Zorn's lemma in general.

In the next section, we prove the above lemma in a fully constructive way, which can be implemented in Haskell.

Using the above lemma, we can complete the proof of Suslin's lemma directly for the case $n \geq 3$ in a constructive way.

Lemma 5.11 (Suslin's lemma for $n \geq 3$) *Let $f = Um_n(R[t])$, with $n \geq 3$ and f_1 monic. Then $I_f = R$. In particular $f(t) \sim f(0)$.*

Proof By lemma 5.10, we can find $c_1, ..., c_m \in R$ and $\Gamma_1, ..., \Gamma_m \in \mathrm{EL}_{n-1}(R[t])$ such that if we denote $g_j = ((f_2, ..., f_n)\Gamma_j)_1$ for $1 \leq j \leq m$, then

$$1 = \sum_j c_j N_{f_1}(g_j)$$

We complete the proof by showing that $N_{f_1}(g_j) \in I_f$ for $1 \leq j \leq m$. But by proposition 5.7, we have $N_{f_1}(g_j) \in \langle f_1, g_j \rangle \cap R$ for $1 \leq j \leq m$. Therefore we may apply lemma 5.9 to see that $N(g_j) \in I_f$. Thus $I_f = R$ and thus $f(t) \sim f(0)$. (Note that lemma 5.9 is constructive.) ∎

6 Completing the construction

6.1 Outline

Recall that we have reduced Quillen-Suslin into Suslin's lemma, constructively. In the previous section, we proved Suslin's lemma in a constructive way, except for lemma 5.10.

In the previous section, we gave a non-constructive proof for lemma 5.10. In this section, we will give a constructive proof which is intended to mimic the non-constructive proof as closely as possible.

All of the constructions here were implemented in the Haskell programming language. For the corresponding Haskell code, see Appendix I.

Notation In this section we use the notation $E_{i,j}(a) = \mathbb{I}_n + a\delta_{i,j} \in \mathrm{EL}_n(R)$ where $i \neq j$, for some $n \geq 2$ and some $a \in R$. Note that $(x_1, \ldots, x_n)E_{i,j}(a) = (x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n)$.

We are also going to need the following corollary. Note that this is a more general version of lemma 5.8 from section 5.3.

Lemma 6.1 *Suppose that $a \in R$. Then $N_q(f + ah) - N_q(f) \in \langle a \rangle$ for any $f, h \in R[t]$.*

Proof In the notation of section 5.3, write $M_{f+ah} = M_f + aM_h$ for the matrix of the linear transformation on $R[t]/\langle q \rangle$ corresponding to multiplication by $f + ah$. Now $N_q(f + ah) - N_q(f) = \det(M_f + aM_h) - \det(M_f)$, which is in $\langle a \rangle$. ∎

Corollary 6.2 *Suppose that $I = \langle a_1, \ldots, a_m \rangle$ is some finitely generated ideal of R. Then given $f, h \in R[t]$ such that $f - h \in I[t]$, we obtain that $N_q(f) - N_q(h) \in I$.*

6.2 Dynamical ideals and induction

Theorem 6.3 *Suppose that for every finitely generated ideal $I \subset R$, we have sets S_I and an ordering $<$ on $S = \{(s, I) \mid s \in S_I\}$, along with a proposition $B(s, I)$ such that for any sequence $(s_1, I_1) > (s_2, I_2) \ldots$ we eventually obtain $B(s_n, I_n)$ for some $n \geq 1$. We are also given some fixed ideal $L \subset R$ and a map $\varphi : \{(s, I) \mid (s, I) \in S, \neg B(s, I)\} \to R$. Suppose that the following holds for every $(s, I) \in S$:*

1. *If $B(s, I)$ then we have $1 \in \langle I, L \rangle$*
2. *If $\neg B(s, I)$, and if either*
   (a) *$\varphi(s, I) \in J$*
   (b) *$1 \in \langle \varphi(s, I), J \rangle$*

   for some ideal $J \supset I$, then there is $s' \in S_J$ such that $(s', J) < (s, I)$.

If the above holds, then given $(s, I) \in S$, we can show $1 \in \langle I, L \rangle$.

Proof We will proceed by induction, using the ordering $<$ and base cases (s, I) such that $B(s, I)$. By 1, the base case $B(s, I)$ is trivial. Now suppose that $\neg B(s, I)$. In this case, there is an element $\varphi(s, I)$ satisfying 2. Since $\varphi(s, I) \in \langle I, \varphi(s, I) \rangle$, we can satisfy 2a. Therefore we obtain $s' \in S_{\langle I, \varphi(s,I) \rangle}$ such that $(s', \langle I, \varphi(s, I) \rangle) < (s, I)$.

We may therefore apply the induction hypothesis to get $1 \in \langle \varphi(s, I), I, L \rangle$.

This shows that we can satisfy 2b, so we get $s'' \in S_{\langle I, L \rangle}$ satisfying $(s'', \langle I, L \rangle) < (s, I)$. Therefore we may apply the induction hypothesis again, to get $1 \in \langle I, L \rangle$. ∎

Note that the above proof is constructive. In the next section we will see that we can obtain a constructive proof of lemma 5.10 by proving the hypothesis of the above theorem constructively.

6.3 Finishing the proof

We now use theorem 6.3 to obtain a constructive proof of lemma 5.10.

Throughout this section, we will fix $f, g \in R[t]^n$, a monic $q \in R[t]$ and $p \in R[t]$ such that $fg = 1 + qp$.

Remark Note that lemma 5.10 is formulated in terms of the unimodular row (q, f). We have chosen to take q out of the row since it doesn't figure algorithmically in the non-constructive proof, which we are trying to mimic here.

In order to use theorem 6.3 we need to define S_I, $<$, $B(s, I)$, $\varphi(S, I)$ and L.

We then need to prove the statements 1, 2, 2a and 2b that are part of theorem 6.3, for our definitions.

Definition 6.4 (S_I and S) *Given an ideal I, we define $S_I = EL_n(R[t]) \times I[t]^n$. Then S is the set of (Γ, h, I) where $(\Gamma, h) \in EL_n(R[t]) \times I[t]^n$ and I is a finitely generated ideal of R.*

Definition 6.5 ($<$ and $B(s, I)$) *Suppose we are given $(\Gamma, h) \in S_I$. Put $f' = f\Gamma - h$. We determine the ordering $<$ by comparing the sum $\sum_{i=1, f'_i \neq 0}^{n} \deg(f'_i)$. We define the statement $B(\Gamma, h, I)$ to be true iff f' has at most one non-zero component. Note note that for infinite sequences $(s_1, I_1) > (s_2, I_2) > \ldots$ we eventually get $B(s_n, I_n)$ for some $n \geq 1$.*

Definition 6.6 (φ) *Given $(\Gamma, h) \in S_I$ such that $\neg B(\Gamma, h, I)$. Put $f' = f\Gamma - h$. Since we assume $\neg B(\Gamma, h, I)$, we may take $\varphi(\Gamma, h, I) = LC(f'_i)$ where i is such that $\deg f'_i = \min\{\deg f'_j \mid f'_j \neq 0\}$.*

Definition 6.7 (L) *We define $L = \langle N_q((f\Gamma)_1) \mid \Gamma \in EL_n(R[t])\rangle$.*

We will now prove 1, 2a and 2b of theorem 6.3.

Lemma 6.8 (1) *Suppose we have $(\Gamma, h) \in S_I$ satisfying $B(\Gamma, h, I)$. Then we have $1 \in \langle I, L\rangle$.*

Proof Since we have $B(\Gamma, h, I)$, $f' = f\Gamma - h$ has at most one non-zero component. If there is one non-zero component in f', then by an elementary transformation we may assume that this is the first component: $f'_1 \neq 0$ and $f'_i = 0$ for all $i > 1$. In either case, we have

$$f'\Gamma^{-1}g = fg - h\Gamma^{-1}g$$

$$f'\Gamma^{-1}g = 1 + pq - h\Gamma^{-1}g$$

$$f'_1(\Gamma^{-1}g)_1 = 1 + pq - h\Gamma^{-1}g$$

$$N_q(f'_1)N_q((\Gamma^{-1}g)_1) = N_q(1 + h\Gamma^{-1}g)$$

Using corollary 6.2 on the right hand side, we obtain $1 \in \langle N_q(f'_1), I\rangle$. We also have $(f\Gamma)_1 - f'_1 = h_1 \in I[t]$ so we again use corollary 6.2 to obtain $N_q(f'_1) - N_q((f\Gamma)_1) \in I$. Thus $1 \in \langle I, N_q((f\Gamma)_1)\rangle \subset \langle I, L\rangle$. ∎

Lemma 6.9 (2a) *Suppose that we have $(\Gamma, h) \in S_I$ such that $\neg B(\Gamma, h, I)$. Suppose also $\varphi(\Gamma, h, I) \in J$ where $I \subset J$. Then we can find $(\Gamma', h') \in S_J$ such that $(\Gamma', h', J) < (\Gamma, h, I)$.*

Proof Put $f' = f\Gamma - h$ and denote $a = \varphi(\Gamma, h, I)$. We may assume that $a = \mathrm{LC}(f'_1)$, since this is possible to arrange by an elementary transformation. Consider $f'' = f' - \mathrm{LT}(f'_1) = f\Gamma - (h + \mathrm{LT}(f'_1))$. Since $a \in J$ we get $\mathrm{LT}(f'_1) \in J[t]$. Since $I \subset J$ we get $h \in J[t]$. Thus $h' = h + \mathrm{LT}(f'_1) \in J[t]$. Clearly, either $f''_1 < f'_1$ or $f''_1 = 0 \wedge f'_1 \neq 0$ holds. Thus $(\Gamma, h', J) < (\Gamma, h, I)$, where $(\Gamma, h') \in S_J$. ∎

Lemma 6.10 (2b) *Suppose that we have $(\Gamma, h) \in S_I$ such that $\neg B(\Gamma, h, I)$. Suppose also $1 \in \langle \varphi(\Gamma, h, I), J\rangle$ where $I \subset J$. Then we can find $(\Gamma', h') \in S_J$ with $(\Gamma', h', J) < (\Gamma, h, I)$.*

Proof Put $f' = f\Gamma - h$ and denote $a = \varphi(\Gamma, h, I)$. As in the proof of the previous lemma, we may assume that $a = \mathrm{LC}(f'_1)$ where $f'_1 \neq 0$. Since $1 \in \langle a, J\rangle$, there is $b \in R$ such that $1 - ab \in J$. Define $\Delta = \prod_{1<i\leq n} E_{1,i}(-b\mathrm{LC}(f'_i)t^{\deg f'_i - \deg f'_1}) \in \mathrm{EL}_n(R[t])$. (Well defined since $\deg f'_1 \leq \deg f'_i$ for all $1 \leq i \leq n$.) Clearly, $(f'\Delta)_1 = 0$ and for $1 < j \leq n$, we have

$$(f'\Delta)_j = f'_j - ab\mathrm{LT}(f'_j)$$

$$(f'\Delta)_j = f'_j - \mathrm{LT}(f'_j) + J[t]$$

Thus if we put $f'' = (f'_1, f'_2 - \mathrm{LT}(f'_2), \ldots, f'_n - \mathrm{LT}(f'_n))$, there is $h' \in J[t]^n$ such that $f'' = f'\Delta - h'$. But $f'' = f'\Delta - h' = f\Gamma\Delta - (h + h')$. Since $I \subset J$ and since $h \in I[t]^n$, we see that $h \in J[t]^n$, so that $h + h' \in J[t]^n$. Thus $(\Gamma\Delta, h') \in S_J$. Since we have at least one non-zero f'_j for some $j > 1$ we obtain either $f''_j < f'_j$ or $f''_j = 0 \wedge f'_j \neq 0$. Thus $(\Gamma\Delta, h', J) < (\Gamma, h, I)$. ∎

Applying theorem 6.3, we now obtain a constructive proof of lemma 5.10 as a corollary.

Corollary 6.11 *We have* $1 \in L$

Proof Apply theorem 6.3 with $(\mathbb{I}_n, (0, \ldots, 0)) \in S_{\langle 0 \rangle}$. ∎

6.4 A note about decidability

The proof in the previous section is constructive, but assumes that equality on R is decidable.

In particular this is assumed when using $<$ to compare elements, and when checking if the base case $B(s, I)$ is satisfied.

It is possible to follow this argument without this decidability hypothesis, in order to obtain the same result for rings R which are not necessarily decidable, thus obtaining a more general result.

For this we consider polynomials in $R[t]$ as sequences of elements in R and we work with the length of this sequence instead of degree of polynomials. If the length of such a sequence is zero, it represents the zero polynomial. This is the algorithm we have implemented in Haskell, which realizes lemma 5.10 in this way for an arbitrary commutative ring R.

7 Appendix A

7.1 Invertible.hs

This is a module for representing rows that are invertible modulo some ideal $(a_1, \ldots, a_m)$. An invertible row consists of the row itself f, its inverse g (a column matrix) and witnesses h of the fact that such that $fg = 1 + (a_1, \ldots, a_m)h$. We represent f, g and h by three lists:

```
module Invertible where

import Algebra.Structures.Ring

data Ring r => Invertible r = Invertible [r] [r] [r]
```

7.2 Transformed.hs

```
module Transformed where

import Algebra.Structures.IntegralDomain
import Algebra.Matrix
import Invertible
import MatrixAux

data Ring r => Transformed r =
  Transformed (Invertible r) (Matrix r) [[r]]

elementary :: IntegralDomain r =>
  r -> Int -> Int -> Transformed r -> Transformed r
elementary q i j (Transformed (Invertible fs gs hs) t hss) =
  let (m,m') = (elemM n q i j, elemM n (neg q) i j) where n = length fs in
  Transformed (Invertible (fs `rmulmat` m) (m' `matmulc` gs) hs)
              (t`mulM`m) (hss `mmulmat` m)

switch :: IntegralDomain r =>
  Int -> Int -> Transformed r -> Transformed r
switch i j
  | i == j = id
  | otherwise = elementary one i j .
                elementary (neg one) j i .
                elementary one i j
```

7.3 DynamicIdeal.hs

```
{-# LANGUAGE GeneralizedNewtypeDeriving #-}

module DynamicIdeal where
```

```
import Control.Monad.Cont
import Control.Monad.State
import Algebra.Structures.Ring
import Invertible
import MatrixAux

runDynamicIdealT (DynamicIdealT prog) invert = do
  evalStateT (runContT prog invert) []

newtype DynamicIdealT r m a =
  DynamicIdealT (ContT (Invertible r) (StateT [r] m) a)
  deriving (Functor, Monad, MonadState [r])

decide :: (Monad m, Ring r) =>
  r -> DynamicIdealT r m (Either [r] (Invertible r))
decide a =
  DynamicIdealT $ ContT $ \k -> do
    as <- get
    let n = length as
    put $ as ++ [a]
    (Invertible xs ys zs'z) <- k $ Left $ basis (length$a:as) (length as)
    let (zs,z) = (init zs'z, last zs'z)
    put $ as ++ xs
    (Invertible us vs wsts) <- k $ Right $ Invertible [neg z] [a]
                                             (zs ++ map neg ys)
    let (ws,ts) = splitAt n wsts
    put $ as
    return $ Invertible (xs ++ us) ((map neg ts) ++ vs) ws
```

7.4 Suslin.hs

```
module Suslin where

import Control.Monad.State
import Control.Monad.Writer
import Algebra.Structures.CommutativeRing
import Algebra.UPoly
import Algebra.Matrix
import Algebra.TypeChar.Char
```

```
import DynamicIdeal
import Invertible
import Transformed
import UPolyAux
import MatrixAux


shed ws dfs (Transformed (Invertible fs gs hs) t hss) = do
  as <- fmap (map liftCoeff) get
  let dhss = (map liftCoeff ws) `ctensorr` dfs
  return $ Transformed (Invertible (fs`rsub`(as`rmulm`dhss))
                       gs (hs`ucsub`(dhss`mmulc`gs))) t (hss`umadd`dhss)

cancel i b row@(Transformed (Invertible fs _ _) _ _) =
  foldr1 (.) [elementary (neg (b<*>(lC f))*>(t<^>((deg f)-(deg$fs!!i))))
                         i j
             |(f,j) <- zip fs [0 ..], f/=zero, j/=i] row

leaf mon r@(Transformed (Invertible fs gs hs) gamma hss) = do
  as <- get
  tell [gamma]
  let (y,x,ws) = (norm mon (head fs), norm mon (head gs),
                  normWitnesses mon one as hs)
      ws' = normWitnesses mon (head fs) as (hss `mmulc` (basis (length fs) 0))
  return$Invertible [y<+>(as`apply`ws')] [x] (ws`cadd`(x`scalec`ws'))

suslin row@(Transformed (Invertible fs _ _) _ _) = do
  let (d,i) = minimum [(deg f,i) | (f,i) <- zip fs [0 ..], f /= zero]
      n = length fs
  if (length$filter (/= zero) fs) == 1
    then return$switch i 0 row
    else do
      ad <- decide$lC$fs!!i
      case ad of
        Left ws -> shed ws ((t<^>d)`scaler`(basis n i)) row >>= suslin
        Right (Invertible [b] _ ws) ->
          (return$cancel i b row) >>=
            shed ws [if j/=i then neg$lT f else zero
                    |(f,j)<-zip fs [0 ..]] >>= suslin
```

```
runSuslin mon fs gs =
  let n = length fs in
  runWriter $ runDynamicIdealT (suslin (Transformed (Invertible fs gs [])
                                  (identity n) [replicate n zero]))
                               (leaf mon)
```

8 Appendix B

We now compute some examples to test the code in Appendix A.

The following examples all take a monic polynomial `monic`, a row `fs` and `gs`, corresponding to q, f and g from section 6.

The output consists of `gammas`, which are matrices over $R[t]$, and `ys`, which are elements of R. They constitute witnesses of the fact that $1 \in L$ where L is as defined in definition 6.7. More precisely; if we denote `gammas` by $\Gamma_1, \ldots, \Gamma_k$ and `ys` by $y_1, \ldots, y_k$, then $N_q((f\Gamma_1)_1)y_1 + \cdots + N_q((f\Gamma_k)_1)y_k = 1$.

8.1 Example 1

This is example 9.2.1 from [Fabianska-Quadrat, 2007].

```
monic: (-5/2)+t
fs: [(13/2),(21/8)]
gs: [5,(-12)]
running suslin...
checking output...
output ok!
gammas:
[[0,(-1/1)]
[1,0]
,[1,(-105/8)]
[0,1]
]
ys:
[21/8,13/2]
```

8.2 Example 2

This is example 9.2.2 from [Fabianska-Quadrat, 2007].

```
monic: ((-2)+u)+t
fs: [(4u+(-2)u^2),(1+4u+(-4)u^2+u^3)]
gs: [((-1/1)+(1/2)u),1]
running suslin...
checking output...
output ok!
gammas:
[[0,((-1/1))]
[1,0]
,[1,(1+(7/2)u+(-6)u^2+3u^3+(-1/2)u^4)]
[0,1]
]
ys:
[1+4u+(-4)u^2+u^3,4u+(-2)u^2]
```

8.3 Example 3

This is example 9.2.3 from [Fabianska-Quadrat, 2007].

```
monic: (2+(-4)u)+t
fs: [((-2)+2u+4u^2),((-1)+2u+4u^2)]
gs: [((-1)),1]
running suslin...
checking output...
output ok!
gammas:
[[0,((-1))]
[1,0]
,[1,((-1)+2u+4u^2)]
[0,1]
]
ys:
[(-1)+2u+4u^2,(-2)+2u+4u^2]
```

8.4 Example 4

This is example 9.2.5 from [Fabianska-Quadrat, 2007].

```
monic: 2xyt+t^2
fs: [x^2t,1+(y^2+2xz)t]
```

```
gs: [((((-4))y^8)+(((-4))y^3+((-16)x)y^6)z+(((-8)x)y+((-16)x^2)y^4)z^2),
     1+((((-1))y^2+((-2)x)y^5)+(((-2)x)+((-4)x^2)y^3)z)t]
running suslin...
checking output...
output ok!
gammas:
[[0,((((-1))))]
[1,0]
,[1,((((-8)x)y^11)+(((-8)x)y^6+((-48)x^2)y^9)z+(((-32)x^2)y^4+
    ((-96)x^3)y^7)z^2+(((-32)x^3)y^2+((-64)x^4)y^5)z^3)]
[0,1]
,[((((-8)x)y^11)+(((-8)x)y^6+((-48)x^2)y^9)z+(((-32)x^2)y^4+
  ((-96)x^3)y^7)z^2+(((-32)x^3)y^2+((-64)x^4)y^5)z^3),((((-1))))+
  ((((-8)x^3)y^11+((-16)x^4)y^14+((-32)x^5)y^17+((-64)x^6)y^20+
  128x^7y^23+256x^8y^26+512x^9y^29)+(((-8)x^3)y^6+((-64)x^4)y^9+
  ((-160)x^5)y^12+((-384)x^6)y^15+((-384)x^7)y^18+2048x^8y^21+4608x^9y^24+
  7168x^10y^27)z+(((-32)x^4)y^4+((-192)x^5)y^7+((-640)x^6)y^10+
  ((-1664)x^7)y^13+256x^8y^16+14336x^9y^19+33792x^10y^22+43008x^11y^25)z^2+
  (((-32)x^5)y^2+((-256)x^6)y^5+((-1280)x^7)y^8+((-3072)x^8)y^11+7680x^9y^14+
  56320x^10y^17+133120x^11y^20+143360x^12y^23)z^3+(((-128)x^7)y^3+
  ((-1280)x^8)y^6+((-1536)x^9)y^9+25600x^10y^12+133120x^11y^15+307200x^12y^18+
  286720x^13y^21)z^4+(((-512)x^9)y^4+2048x^10y^7+38912x^11y^10+188416x^12y^13+
  417792x^13y^16+344064x^14y^19)z^5+(2048x^11y^5+28672x^12y^8+147456x^13y^11+
  311296x^14y^14+229376x^15y^17)z^6+(8192x^13y^6+49152x^14y^9+98304x^15y^12+
  65536x^16y^15)z^7)t]
[1,((x^2+2x^3y^3+4x^4y^6+8x^5y^9+((-16)x^6)y^12+((-32)x^7)y^15+((-64)x^8)y^18)+
(4x^4y+16x^5y^4+16x^6y^7+((-128)x^7)y^10+((-320)x^8)y^13+((-512)x^9)y^16)z+
(16x^6y^2+((-32)x^7)y^5+((-384)x^8)y^8+((-1152)x^9)y^11+((-1536)x^10)y^14)z^2+
(((-64)x^8)y^3+((-512)x^9)y^6+((-1792)x^10)y^9+((-2048)x^11)y^12)z^3+
(((-256)x^10)y^4+((-1024)x^11)y^7+((-1024)x^12)y^10)z^4)t]
]
ys:
[(1+((-2)x)y^3)+(((-4)x^2)y)z,0,(1+((-2)x)y^3+16x^4y^12)+(((-4)x^2)y+
 16x^4y^7+96x^5y^10)z+(64x^5y^5+192x^6y^8)z^2+(64x^6y^3+128x^7y^6)z^3]
```

8.5 Example 5

This is example 9.2.6 from [Fabianska-Quadrat, 2007].

```
monic: t^2
fs: [(1+3u),u^2+(1+u)t]
gs: [(1+(-3)u)+((-9)+18u)t,9+((-54))t]
running suslin...
checking output...
output ok!
gammas:
[[0,((-1))]
[1,0]
,[((-1)+2u+(-6)u^2+18u^3+27u^4)t,((-1))]
[1,0]
,[1,((-1)u^2+3u^3+(-9)u^4+27u^5)+((-1)+2u+(-6)u^2+18u^3+27u^4)t]
[0,1]
]
ys:
[u^4,u^4,1+6u+9u^2]
```

9 Index of notations

R	a commutative ring with a 1
k	a field
$\mathrm{LC}(f)$	leading coefficient of the polynomial f
$\mathrm{LT}(f)$	leading term of the polynomial f
$\deg f$	degree of the polynomial f
$\mathfrak{M}(R)$	the collection of finitely generated R-modules
$\mathfrak{B}(R)$	the collection of finitely generated, projective R-modules
$A \twoheadrightarrow B$	surjective homomorphism from A to B
$A \xrightarrow{\sim} B$	isomorphism from A to B
$\mathrm{Um}_n(R)$	the set of all unimodular rows of length n, over R
$\mathfrak{F}(R)$	the collection of all free R-modules
$\mathfrak{F}_s(R)$	the collection of all stably free R-modules
$\mathrm{GL}_n(R)$	the general linear group of degree n over R
$\mathrm{SL}_n(R)$	the special linear group of degree n over R
$\mathrm{EL}_n(R)$	the group of elementary transformations of degree n over R
$\mathbb{I}_n$	$n \times n$ identity matrix

References

Serre, Jean-Pierre (March 1955), "Faisceaux algébriques cohérents", *Annals of Mathematics. Second Series. 61 (2): 197–278*

Serre, Jean-Pierre (1958), "Modules projectifs et espaces fibrés à fibre vectorielle" (in French), *Séminaire P. Dubreil, M.-L. Dubreil-Jacotin et C. Pisot, 1957/58, Fasc. 2, Exposé 23*

Ernst Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser Boston, 1985.

Ihsen Yengui, Henri Lombardi, *Suslin's algorithms for reduction of unimodular rows*. 2005.

Tsit Yuen Lam, *Serre's Problem on Projective Modules*. Springer Monographs in Mathematics, 2006.

Anna Fabiańska, Alban Quadrat *Applications of the Quillen-Suslin theorem to multidimensional systems theory*. INRIA, 2007.